DIR Cybersecurity Insight

Newsletter

May FY2015 | DIR OCISO | DIRSECURITY@DIR.TEXAS.GOV

2015 Information Security Forum Coming Soon!

The Information Security Forum has been a premier event for IT professionals, and this year continues in the tradition of excellent content and great networking possibilities.

We have made several changes to this year's conference, continuing the evolution of this premier event. Changing the venue, expanding the agenda to allow for multiple session tracks, and inviting local governments to attend will all provide more opportunities for learning and sharing than in years past.

The keynote speakers this year are dynamic interesting people with unique views on information technology and security. The session tracks on day one highlight current events and trends in information security – Security Operations, Governance, Vulnerability Management, Threat Landscapes, and Managing Compromise will provide insight and fresh ideas you can bring back to your organization. The workshops on day two include both classroom-style and hands-on learning opportunities.

Click here to view more information on the 2015 DIR ISF! See the agenda for more information about the tracks.

Contents

NEWS!

State of Texas Cybersecurity Coordinator Named

AUSTIN: The Texas Department of Information Resources (DIR) announced the promotion of Edward Block to serve as the State of Texas Chief Information Security Officer (CISO). Edward brings years of experience at DIR in cybersecurity management, having most recently served as Interim CISO since February. His new responsibility begins immediately.

As leader of the state's Chief Information Security Office, Edward will oversee management of statewide security programs and coordinate Texas public-sector cybersecurity efforts. The Office provides security services, policy and assurance, risk management, and education and training to Texas public-sector government organizations. While the CISO serves all Texans, the position resides at DIR.

"Edward has been instrumental in building Texas' Chief Information Security Office into a highly functioning program that serves our customers in a very prolific way," said DIR Interim Executive Director Todd Kimbriel. "I am looking forward to his continuing efforts to make this program the best in the nation."

Eddie Block
CISO, State of Texas

The CISO also serves as the state's cybersecurity coordinator and is responsible for strengthening the cybersecurity culture within Texas. In this role, the CISO brings together both private industry and public-sector organizations to develop and encourage wider adoption of cybersecurity best practices to protect critical state infrastructure and sensitive information. The cybersecurity coordinator role also drives education and skill-building efforts to produce an exemplary cybersecurity workforce within the state.

"Texas should serve as an example of information security done right. We have done a great amount of work over the past two years, but the job is far from complete," said Edward. "As the threats against state information resources evolve, we have to be prepared to look at new technologies, new processes, and new controls that balance the needs of the state's business with the risks we all face. We must work together to create the environment that our citizens deserve."

Edward has been with DIR in the role of Deputy CISO for the State of Texas since 2012. Edward is a licensed member of the State Bar of Texas, admitted to the U.S. District Court, Western District of Texas, and Chairs the Austin Bar Association's Technology Law Section. He is also a Certified Information Systems Security Professional (CISSP), Certified Information Privacy Manager (CIPM), Certified Information Systems Auditor (CISA), and Certified Ethical Hacker (CEH).

Edward is also a graduate of the St. Mary's University School of Law and Loyola-Marymount University.

Spring Learning

Spring is the time of year that, when we were students, we were counting down the days until summer. That last two months was the toughest stretch of school to get through. We were already looking forward to no school, no homework, and no learning for three months.

As we get older, we realize that learning is a never-ending process. The more we learn, the better we do in our personal and professional lives. Even though we may not always have a stockpile of time or money to focus strictly on education, we grab those opportunities as they come our way.

DIR is currently offering several learning opportunities, both ongoing, and in the coming weeks. These opportunities are free to state agencies and are reasonable in length:

- DIR Information Security Forum (May 20-21) – This is an educational conference for IT professionals that focuses on topics relating to security. This is a two-day conference with five tracks of breakout sessions on day one and workshops on day two. This is a fun and informational conference that can help you improve programs at your organization. Registration is limited, but space is still available! Click here to register. If you have questions, contact ISF@dir.texas.gov.

- InfoSec Academy – The InfoSec Academy attendance continues to grow. The courses offered can help you prepare for a certification, such as the CISSP. Soft skills courses are also available. Currently, the InfoSec Academy is offering a Policy and Assurance Course that discusses the new TAC 202, the new Security Framework, and more. This is a one-day course and is offered at no cost to ISOs. See the article later in this newsletter for more details. If you have questions about the InfoSec Academy, contact InfoSecAcademy@dir.texas.gov.

- Gartner Research Licenses – DIR is offering licenses to state agencies and institutions of higher education for the Gartner Research Library. This is a comprehensive collection of white papers and articles on all things IT-related. If you are not sure if you have a license, contact DIRSecurity@dir.texas.gov.

- Securing the Human End User Training Program – In the continuing effort to support your agency security program, the OCISO has purchased Securing the Human End User training for State of Texas employees via the SANS Institute.
- Securing the Human End User training focuses on daily challenges, including topics such as social engineering threats, safe web browsing, and the importance of using strong passwords. This computer-based training is designed to increase your users' security awareness by adding elements to help modify online behavior. More than 40 modules are available. To initiate the registration process, contact dirsecurity@dir.texas.gov. Visit www.securingthehuman.org to learn more about Securing the Human.

In addition, several free webinars are offered throughout the year. These webinars range from how to use Microsoft Office products more efficiently to creating meaningful metrics in an information security program. Subscribing to the various mailing lists will ensure you get these notifications.

KEEP LEARNING
learn, teach, share

Don't let spring be a tough stretch. Taking advantage of these opportunities is a worthwhile venture that can not only fuel the need to learn but can also help you make a difference!

Network Security Operations Center (NSOC)

Got .com headaches? You may not realize that your agency is buying domain registration and hosting services from discount registrars for .com, .net, .org, etc., domains. And they have a good reason to do so. DIR only provides registration services for the .gov top level domains (TLD). Agencies are forced to go elsewhere to register these other TLD domains, and they are using them more and more. With the growth of web-based communications, it is becoming common practice to register an associated TLD domain name as part of an overall communications effort. That makes it easier for users to find specific information and easier for agencies to track the effectiveness of their communications campaign. And let's face it, $8.oo a year for this type of service is hard to beat.

However, in practice, this outside hosting can cause headaches. Why? To understand why there is a problem, we first need to understand why it is necessary to use outside hosting and how it actually works.

Your agency has a pressing communication issue, and their efforts are focused around a campaign to notify the public of Issue Awareness. So they register www.IssueAwareness.com and host it with StopMomma.biz. The actual website and all content is being developed in-house and actually resides on www.YourAgency.Texas.gov as a sub-site. This is great because it lives in your environment.

So far, so good. So why even pay for hosting if the site lives on your current web server? When you register a domain name, a DNS record is created that resolves IssueAwareness.com to an IP address. If your agency just buys the domain name, the DNS record would have to resolve to the same IP as www.YourAgency.Texas.gov and hence, visitors would land on the home page and then have to navigate to the IssueAwareness.com page. This makes tracking visitors and campaign effectiveness difficult.

However, if you take advantage of HTTP standards, you can use 301-Redirection in a single small, one-file website on StopMomma to redirect browser requests to a specific URL on www.YourAgency.Texas.gov. The user never sees anything load from the StopMomma-hosted computer. Instead, the StopMomma site acts as a pass-through, sending the user directly to the agency's specified page for Issue Awareness. Visitors see www.IssueAwareness.com in their browser and can now directly access the information they want, and your agency can also track the effectiveness of the campaign.

Again so far, so good. But this is where the headaches start.

When your agency takes advantage of this cheap registration and hosting option, their IssueAwareness.com domain is placed on a

shared server with hundreds or even thousands of other domains. All of these domains share the same IP address. And often, security tools and intelligence is based on IP addresses. So if one website is compromised or if another customer is an outright criminal, the IP address can be tagged as malicious. Once an IP is tagged as malicious, security tools (IPS, MPS) and teams will start to block their users from accessing the bad IP address regardless of which website on that server they want to visit. ISPs and other businesses or agencies do not want to expose users to that risk. Once blocks are activated, users can no longer access www.IssueAwareness.com. This is worth noting because it is at risk of being blocked not only by the NSOC but also by any IT shop providing security to their enterprise.

Here at the NSOC, we will block a StopMomma.biz server if it is involved in malicious activity like malware delivery. Then the agency hosting their .com domain on that server can no longer access that website. Once that happens, employees on the state network cannot access the website using www.IssueAwareness.com, but they can still access it directly using www.YourAgency.texas.gov/campaigns/IssueAwareness/index.html. This may also be true for corporate visitors whose network security actively blocks malicious actors. Users connected via open networks like coffee shop Wi-Fi or smart phones will NOT be affected.

What are your options if DNS alone can't solve it and hosting at discount webhosts is a security/access risk? One solution is to pay for a dedicated server to host www.IssueAwareness.com. Another option is to stand up your own shared server configured like a webhost to resolve several domains on the same IP address. Or you can continue to use the StopMommas, but be aware that you may have to deal with a few future headaches. Hopefully more options will be available eventually.

If you think your site is being blocked by the NSOC, contact the NSOC helpdesk at nsoc-helpdesk@nsoc.dir.texas.gov to confirm. If we are in fact blocking, we will work with you to determine a proper course of action. Keep in mind that any action taken by the NSOC will only affect employees on the state network. This will not

prevent other companies from blocking that IP address/website. This includes considering the residual risk of infection to you and your customers that may occur from visiting sites hosted on these malicious serve.

Jeremy A. Wilson
DIR Security Operations Center Manager

Information Security Officer Spotlight

Thuy Cao, CISSP
Information Security Officer and Continuity of Operations Planning Officer Texas Commission of Environmental Quality

I was born and raised in Saigon, Vietnam. My parents coached me early on about the importance of education. When I moved to the United States at the age of eighteen, I wanted to pursue my career in IT. I graduated from California State University, Fullerton, with a BA Degree in Business Administration, concentrating on MIS.

How did you come to the security field?
After graduating, I worked for a leading company in the field of IT as a system administrator. Part of my job was to be compliant with security policy, working closely with the system security auditing team. My lasting impression during those routine audits was the auditor's vast knowledge and comprehension in the field of IT. I want to be that person. My career path was clear by then. With management support, I transitioned into the System Security Analyst role. After joining TCEQ, I was given an opportunity to follow my passion; I became an ISA and then was promoted to be the agency ISO.

Tell us how information security has changed since you started in your role.
Information security plays an important role in any organization. Executive management's increasing support over the years regarding the need for an information security program and allocating much needed resources for ongoing information security implementation, remediation, and compliance activities has been a welcome change in this field.

Who are your users/customers, and what is one of the most challenging areas for you?
Our customers are internal staff, contractors, and the general public.

The biggest challenge for me is educating and training non-technical people to protect their workstations. My daily advice to internal staff is to observe the agency's compliance and use IT resources safely and responsibly.

How did you learn about TCEQ?
I have friends who have worked for TCEQ for almost two decades and have been impressed with its impact to our daily lives.

What do you like best about your job?
The support I receive from my executive management on information security. The opportunity for me to further my knowledge, my career in this field. The talented and dedicated members of this department, this agency that I have the opportunity to work with.

What would people never guess you do in your role?
I am also a Professional Continuity Practitioner.

What other career would you have liked to pursue?
If I had another choice, I would like to pursue an opportunity in Healthcare Administration.

Have you ever changed career paths?
I have thought about it at checkpoints in my career. But I find it more compelling every day. I believe I made the right choice for my career.

What has been the greatest challenge that you have faced, and how did you resolve it?

Building trust from my team members. It took dedication, commitment to team building, non-stop learning, and hard work to prove my worth to the business. And most of all continue to maintain my team's trust.

Tell us about your most proud accomplishment.
I believe my most proud accomplishment is still in front of me, in the very near future.

Top 3 life highlights?
Becoming a US citizen

Marrying my high school boyfriend
Giving birth to my two wonderful sons.

Where did you grow up?
I spent 18 years in Saigon, Vietnam, and the next eight years in Southern California.

Do you have family in Austin?
Yes, my husband, 2 kids, my parents, and parents-in-law.

What are your hobbies?
Reading and watching movies – anything related to Mother Nature, zombies, and science fiction.

Spending quality time with my family.

People would be surprised to know that you…
I believe my friends and family know me very well. No surprises here.

Are you messy or organized?
Very organized

Favorite travel spot?
Hawaii

What was the last book you read?
Divergent Trilogy

What radio station do you listen to?
96.7

If you could interview one person (dead or alive) who would it be?
Karen Robinson

If you had to eat one meal, every day for the rest of your life, what would it be?
Rice

Least favorite food?
None, I like everything that is edible.

If given a chance, who would you like to be for a day?
I would like to be in my Deputy Director's shoes for one day.

If you were to write a book about yourself, what would you name it?
My Journey in America – The Land of Freedom and Opportunity

Describe what you were like at age 10.
Thin and very shy

What is one thing you couldn't live without?
Family

What is your hidden talent?
I believe it is persuasion.

What is the best advice you have received and that you have used?
Treat people the way you want to be treated.

What would be your advice for a new security professional?
You will learn a lot from working and networking with people in the field.

Program Updates

Texas InfoSec Academy

Texas Security Policy & Assurance Course Available Now

The InfoSec Academy is offering the Texas Security Policy & Assurance course. CISOs and ISOs of state agencies and institutions of higher education are required to take this course. This course is designed to prepare attendees to apply the Texas rules regarding information security within their organizations. The course will cover Texas Rules and Regulations, data classification, the Texas Cybersecurity Framework, agency security plans, and reports. Course dates & locations are as follows:

Date	Location
May 11, 2015	William P Clements – 301 W. 15th, Austin, Texas; Room 205
May 12, 2015	William P Clements – 301 W. 15th, Austin, Texas; Room 205
May 21, 2015	Palmer Events Center, 900 Barton Springs Rd, Austin, TX 78704 Note: This class is held on the last day of the Information Security Forum and is designated for out-of-town attendees.

Space is limited. Login to the InfoSec Academy LMS to register.

If you have any questions about the Texas InfoSec Academy, email infosecacademy@dir.texas.gov or call Michele Elledge at 512-475-0419.

Archer GRC Portal

The adoption rate of the Archer Incidents System has been outstanding. In March, we enabled a new feature which allows the NSOC to send incident information directly to you via Archer including issues that have been identified through perimeter devices, MS-ISAC notifications, etc. In addition, when we see password dumps or other potential issues on Pastebin.com, we will distribute those via Archer.

We are currently working on the ISAAC risk assessment system replacement. Many security professionals from several agencies and institutions of higher education are working with us to ensure that it will meet your needs. We plan to release it at the DIR Information Security Forum in May. Additionally we will be sending an email to the ISO's and CISO's with an attached Excel template. The template will enable you to give us information on your applications, data centers, networks, and new users for Archer. We will be able to upload this information for you, which will save you time and data entry in the future if you plan to use the new risk assessment system.

Once the risk assessment portion is complete, we will work with the Information Resource Deployment Review (IRDR) team to potentially use the Archer GRC Portal to gather that information.

If you have questions or suggestions regarding the Archer GRC Portal, please contact us at grc@dir.texas.gov.

MANY THANKS TO THE SISAC RISK ASSESSMENT SUBCOMMITTEE FOR THEIR WORK TO DATE. COMMITTEE MEMBERS INCLUDE:

Kevin Kjosa, Co Chair - University of Texas System

Darrell Bateman - Texas Tech University

Kent Dyer - Texas Department of Licensing and Regulation

Shirley Erp – Health and Human Services Commission

Dave Gray - Comptroller of Public Accounts

Ann Hallam - State Office of Risk Management

Mark Herber - Department of Family and Protective Services

Jeff McCabe - Texas A&M University

Arturo Montalvo - Office of Attorney General

Matt Riemersma - Department of Assistive and Rehabilitative Services

Brandon Rogers - General Land Office

Charlotte Russell - University of North Texas System

Shenny Sheth - Department of Aging and Disability Services

Khatija Syeda - Health and Human Services Commission

Lisa Wei - Comptroller of Public Accounts

Robert Myles - Symantec

Insight from our Texas CISO

It seems to be more and more common to hear of massive data breaches — 100,000 student transcripts,[1] 56 million credit cards,[2] 78 million health records,[3] the reports just keep coming. On one level there is the very real risk that consumers will get weary of the reports and stop paying attention. I remember thinking, when the HI-TECH revisions to HIPAA first appeared with a mandatory reporting requirements for breaches over 500 records and a public "website of shame," that it would be painful to be the first on the list but not the 100th. If you look at the HHS website today (1171 breaches at the time of this article)[4] it is easy for a single breach to get lost in the noise.

Eddie Block
CISO, State of Texas

That weariness goes both ways, though. Consumers, many of whom also utilize state services, may start to expect more from those who hold their data. Take the recent Premera Blue Cross[5] breach as an example. Consumers are not satisfied with an indefinite statement like, "Your data may have been exposed." They are looking for solid answers like the aspects of PII that are at risk, who the attackers were, and how long the entity has known about the breach. And they want those answers quickly.

Like consumers, regulators are starting to pay attention to how long breach disclosures take. In the Premera breach, the Washington State Insurance Commissioner publically stated that he was concerned with how long Premera took to notify the state[6] and has opened an investigation with Alaska and Oregon into the issue.[7]

Consumers are also questioning the security controls that led to the breach. In the wake of the recent Premera Blue Cross announcement, Jeffrey Carr, President and CEO of Taia Global (a security firm) and a Premera customer, penned an interesting response[8] to Premera's CEO. According to Carr, Premera received a report from the U.S. Office of Personnel Management's Office of the Inspector General weeks before the breach indicating distinct security issues:

- Premera was slow to patch, leaving systems vulnerable to attack.
- Premera used unsupported software, for which patches were not available.
- Premera had servers that were found to be insecure in vulnerability tests.

How many state entities do these same statements apply to?

Earlier this month, DIR began circulating a draft Software Currency policy to DCS agencies in an attempt to address the type of issue Premera had with their unsupported systems. After systems go out-of-support, security holes are left open potentially forever. Attackers understand this all too well. When Windows XP went out-of-support last year, there were reports of vulnerabilities being held back from disclosure until after the end of support date, so that they would never be patched.

As trusted custodians of citizen data, it is our responsibility to not only protect the data we have been entrusted with, but also to ensure that we are prepared to react in the event of a breach. Knowing that it can take days to develop public statements, it is important to have draft language available before any breach takes place. We can't simply issue generic, boilerplate language, however. We need to ensure that our citizens are given sufficient information to assess their own risk and deliberate actions they can take to protect their identity.

Eddie Block
CISO, State of Texas

---

[1] http://www.scmagazine.com/transcript-website-flaw-exposed-personal-data-on-98k-users/article/378787/
[2] http://www.pcworld.com/article/2852472/home-depot-spent-43-million-on-data-breach-in-just-one-quarter.html
[3] http://www.csoonline.com/article/2888307/data-protection/anthem-78-8-million-affected-fbi-close-to-naming-suspect.html
[4] https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf
[5] http://www.reuters.com/article/2015/03/17/us-cyberattack-premera-idUSKBN0MD2FF20150317
[6] http://thehill.com/policy/cybersecurity/236002-regulator-dings-premera-over-breach-notification-wait
[7] http://stateofreform.com/news/states/alaska/2015/03/wa-washington-to-lead-multi-state-investigation-of-premera-hack/
[8] http://jeffreycarr.blogspot.com/2015/03/open-letter-to-premera-blue-cross-ceo.html?utm_content=buffer47f2b&utm_medium=social&utm_source=twitter.com&utm_campaign=buffer

Events

Training and Conferences Around the State

Monthly Security Program Webinar
Selecting the Right Identity Governance and Administration tool for the Job!
Date: May 12, 2015 at 2:00 PM CDT.
Time: 2:00 pm CDT

Register now! https://attendee.gotowebinar.com/register/1438907044175098881

Date: Wednesday – Thursday, May 20 – 21, 2015
Time: 8:00 – 4:30
Place: Palmer Events Center
             900 Barton Springs Road
             Austin, TX 78704

Registration is open!
Visit the website for more information.

2015 Save the Dates

- BSides San Antonio May 10
- ISO 27001 summit, May 13 – 14
- NSA Information Assurance Directorate's (IAD) Information Assurance Symposium (IAS): June 29 – July 1 Washington, D.C.
- Blackhat USA, August 1 – 6
- TASSCC Annual Conference, August 2 – 5; La Cantera Resort, San Antonio
- BSides Las Vegas, August 5 – 6
- Defcon 23 August 6 – 9
- LASCON 2015, October 19 – 22:
- Dallas Secure World, October 28 – 29, 2015

IN SPECIAL MEMORY OF: KEN PALMQUIST.

Readers of our February 2015 issue will remember our ISO spotlight on Ken Palmquist, the ISO for DIR. We are saddened to say that Ken passed away April 10 at home on his acreage outside Lexington, Texas. Ken was an important member of the Texas information security community and will be missed.

February's newsletter

Feedback, comments, stories, etc.
DIRSecurity@dir.texas.gov

Office of the
CHIEF INFORMATION
SECURITY OFFICER
State of Texas